ABSTRACT OF THE DISCLOSURE

METHOD AND SYSTEM FOR A FLEXIBLE LIGHTWEIGHT PUBLIC-KEY-BASED MECHANISM FOR THE GSS PROTOCOL

A method for establishing a secure context for communicating messages between a client and a server is presented that is compliant with the Generic Security Service application programming interface (GSS-API). The client sends to the server a first message containing a first symmetric secret key generated by the client and an authentication token; the first message is secured with the public key from the server's public key certificate. After the server authenticates the client based on the authentication token, the client then receives from the server a second message that has been secured with the first symmetric secret key and that contains a second symmetric secret key. The client and the server employ the second symmetric secret key to secure subsequent messages sent between the client and the server. The authentication token may be a public key certificate associated with the client, a username-password pair, or a secure ticket.